UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Search of

INFORMATION ASSOCIATED WITH THE GOOGLE ACCOUNT jimmygoings50@gmail.com THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC.

Case No. 4:23-MJ-7292 SPM

SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRONIC MEANS

APPLICATION FOR A SEARCH WARRANT

I, Stephanie Stoehner, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A

located in the NORHTERN District of CALIFORNIA, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section - Offense Description

18 USC Sections 2252A(a)(1), knowingly mailing, transporting, or shipping child pornography in interstate or foreign commerce by any means; 2252A(a)(2)(A) knowingly receiving or distributing any child pornography that has been mailed or shipped or transported in interstate or foreign commerce by any means; and 2252A(a)(5)(B) possessing any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under the penalty of perjury that the foregoing is true and correct.

Del Stoehner 3932

Applicant's signature

Stephanie Stoehner, SFO

Printed name and title

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41

Date: 08/04/2023

Judge's signature

City and state: St. Louis, MO

Honorable Shirley Padmore Mensah, U.S. Magistrate Judge

Printed name and title

AUSA: NATHAN CHAPMAN

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE GOOGLE ACCOUNT jimmygoings50@gmail.com THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC.	No. 4:23-MJ-7292 SPM SIGNED AND SUBMITTED TO THE COURT FOR FILING BY RELIABLE ELECTRONIC MEANS **FILED UNDER SEAL**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR SEARCH WARRANT

I, Stephanie Stoehner, being duly sworn via reliable electronic means, do hereby depose and state:

INTRODUCTION

1. This affiant is a detective with the St. Louis County Police Department and a Special Federal Officer with the Federal Bureau of Investigation (FBI). This affiant has been employed with the St. Louis County Police Department since January of 2010 and a sworn Police Officer since December of 2010. This affiant is currently assigned as a detective in the Division of Criminal Investigation, Bureau of Crimes Against Persons, Special Investigations Unit. This affiant has been involved in numerous investigations involving the exploitation of children, the use of the Internet to induce a minor to engage in a criminal sexual offense, and the dissemination of child pornography on the Internet via computer. This affiant has attended specialized courses involving computer crime investigations, child exploitation, and undercover online investigations. This affiant has been personally involved in the execution of search warrants to search residences and seize material relating to the sexual exploitation of minors

including computers, computer-related equipment, software, and electronically-stored information.

2. This affidavit is made in support of an application for a search warrant to search for and seize instrumentalities, fruits, and evidence of violations of Title 18, United States Code, Sections 2252 and 2252A, which criminalize, among other things, the possession and/or receipt and shipment of child pornography, and other related materials. The items that are the subject of the search and seizure applied for in this affidavit are more specifically described in Attachment A.

3. The statements contained in this affidavit are based on this affiant's personal knowledge or information provided to this affiant by other law enforcement officers and other agencies. Since this affidavit is being submitted for the limited purpose of securing a search warrant, this affiant has not included each and every fact known to me concerning this investigation. This affiant has set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of Title 18, United States Code, Sections 2252A(a)(2), and 2252A(a)(5)(B), including but not limited to the items described on Attachment A, which is attached hereto and incorporated herein by reference, will be found within the following Google account of **James Goings**, aka "**jimmygoings50@gmail.com**."

STATUTORY AUTHORITY

4. This investigation concerns alleged violations of Title 18, United States Code, Section 2252A, relating to the sexual exploitation of minors. Title 18, U.S.C., § 2252A(a)(2)(A) prohibits a person from knowingly receiving or distributing any child pornography that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing any book,

magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in interstate or foreign commerce by any means, including by computer.

DEFINITIONS

5. The following definitions apply to this Affidavit and Attachment A to this Affidavit:

a. "Child erotica" are materials or items that are sexually arousing to pedophiles but that are not in and of themselves obscene or which do not necessarily depict minors in sexually explicit poses or positions.

b. "Child pornography," as used in this affidavit, includes the definition in Title 18, USC, Section 2256(8)(A) and (C), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct.

c. 18 U.S.C. § 2256(5) states: "'visual depiction' includes undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image."

d. The term "computer," as used herein, is defined pursuant to Title 18, United States Code, Section 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

e. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit

electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

f. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. "Computer-related documentation," as used herein, consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

h. "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might be static whereby the user's ISP assigns his computer a unique IP address – and that same number is used by the user every time his computer accesses the Internet. Numerical IP addresses generally have corresponding domain names. For instance, the IP address 149.101.10.40 traces to the corresponding domain name "www.cybercrime.gov". The Domain Name System or DNS is an Internet service that maps domain names. This mapping function is performed by DNS servers located

throughout the Internet. In general, a registered domain name should resolve to a numerical IP address.

i. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

j. "Computer passwords" and "data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

k. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, genital-anal, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

l. "Internet addresses" take on several forms, including Internet Protocol (IP) addresses, Uniform Resource Locator (URL) addresses, and domain names. Internet addresses are unique and can be traced to an identifiable physical location and a computer connection. The Internet Protocol address (or simply "IP" address) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.187). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP address acts much like a home or business street address, it enables Internet sites to properly route traffic to each other. The assignment of IP addresses to computers connected to the Internet is controlled by ISPs. There are two types of IP addresses, dynamic and static. To assign dynamic IP addresses, the ISP randomly assigns one of the available IP addresses, in the range of IP addresses controlled by the ISP, each time a customer dials in or connects to the ISP in order to connect to the Internet. The customer's computer retains that IP address for the duration of that session (i.e., until the user disconnects), and the IP address cannot be assigned to another user during that period. Once the user disconnects, that IP address becomes available to other customers who dial in at a later time. Thus, an individual customer's dynamic IP address may, and almost always will, differ each time he dials into or connects to the ISP. To assign static IP addresses, the ISP assigns the customer a permanent IP address. The customer's

computer would then be configured with this IP address every time he dials in or connects to the ISP in order to connect to the Internet.

m. The "Internet" is a collection of computers and computer networks which are connected to one another via high-speed data links and telephone lines for the purpose of sharing information. Connections between Internet computers exist across state and international borders and information sent between computers connected to the Internet frequently crosses state and international borders, even if those computers are in the same state. A network is a series of devices, including computers and telecommunication devices, connected by communication channels.

n. An "internet service provider" (ISP) is a commercial service that provides Internet connectivity to its subscribers. In addition to providing access to the Internet via telephone lines or other telecommunications lines, ISPs may also provide Internet e-mail accounts and other services unique to each particular ISP such as Usenet Newsgroups and Internet Relay Chat. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with it. Those records could include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, customer service information and other information, both in computer data format and in written record format.

o. A "server" is a centralized computer that provides services for other computers connected to it via a network. The computers that use the server's services are sometimes called "clients".

STORED WIRE AND ELECTRONIC COMMUNICATION ACCESS

6. Title 18, United States Code, Sections 2701 through 2711, is entitled "Stored Wire and Electronic Communications and Transactional Records Access."

a. Title 18, United States Code, Section 2703(a) provides, in part:

> A governmental entity may require the disclosure by a provider of electronic communication service the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure by a Court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

b. Title 18, United States Code, Section 2703(b) provides, in part:

> (1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection –
>
> > (A) Without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the procedures described in the Federal Rules of Criminal Procedure by a Court with jurisdiction over the offense under investigation or equivalent State warrant...

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service: –

(A) On behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) Solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

c. The government may also obtain records and other information pertaining to a subscriber or customer of electronic communication service or remote computing service by way of a search warrant. 18 U.S.C. § 2703(c). No notice to the subscriber or customer is required. 18 U.S.C. § 2703(c)(2).

d. Title 18, United States Code, Section 2711, provides, in part:

As used in this chapter –

(1) The terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and

(2) The term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.

e. Title 18, United States Code, Section 2510, provides, in part:

(8) "Contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication; . . .

(14) "Electronic communications system" means any wire, radio, electromagnetic, photo-optical or photo-electronic facilities for the transmission of wire or electronic communications and any computer facilities or related electronic equipment for the electronic storage of such communications; . . .

(15) "Electronic communication service" means any service, which provides to users thereof the ability to send or receive wire or electronic communications; . . .

(17) "Electronic storage" means –

a. Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

b. Any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

AGENT BACKGROUND AND INVESTIGATION

7. This affiant has been employed as a police officer for approximately thirteen years and is currently assigned as a detective to the Division of Criminal Investigation's Special Investigations Unit with the St. Louis County Police Department. During the course of this time period, this affiant has had numerous contacts and dealings with informants, other police officers, individuals known to possess and sell obscene material, as well as subjects known to possess, distribute, and manufacture child pornographic images and/or videos. This affiant has received specialized training in the area of computer-based investigations. This affiant has also

received training in the area of internet crimes against children from the National Center for Missing and Exploited Children (NCMEC), as well as attended the Internet Crimes Against Children's (ICAC) Investigative Techniques Training Program, the ICAC Online Ads Training Program, and the ICAC Undercover Investigations Training Program. This affiant has assisted in numerous investigations and search warrants relative to the crimes of manufacturing, possession, and distribution of child pornography. This affiant is also familiar with investigating Cyber-Tip reports, conducting on-scene interviews, and "knock and talk" investigation techniques.

8. The statements in this affidavit are based in part on this affiant's personal knowledge or information provided by other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, this affiant has not included each and every fact known to her concerning this investigation.

9. On April 4th, 2022, Sergeant Brian Shanika, DSN 2976, of the St. Louis County Police Department's Special Investigations Unit, advised this affiant that CyberTipline Report #112013929 from the National Center for Missing and Exploited Children (NCMEC) had been forwarded to the Special Investigations Unit. The CyberTipline Report was reported to NCMEC on December 23rd, 2021, at 03:03:43 hours (UTC) by Google.

10. The CyberTipline Report advised that the Google account registered with the name "Jim," verified telephone number of (314) 666-0429, date of birth of xx-xx-1998, verified email address of "jimmygiongs50@gmail.com," and additional email address of "jimmygoings50@yahoo.com," was used to upload four (4) files depicting child pornography / child sexual abuse material (CSAM). The CyberTipline indicated that the account was accessed from the IP address of 2600:1700:acaf:b000:58c3:9d3a:6ae7:9830 on December 16th, 2021 at 00:49:49: hours (UTC).

11. NCMEC reported through Geo-Lookup that the IP address 2600:1700:acaf:b000:58c3:9d3a:6ae7:9830 is listed as belonging to AT&T Uverse, and registered within the St. Louis metropolitan area.

12. On March 8th, 2022, a subpoena was sent to AT&T Internet Services for user/subscriber information, to include method and type of payment for the IP address of 2600:1700:acaf:b000:58c3:9d3a:6ae7:9830 assigned on December 16th, 2021, at 06:33:20 hours (GMT). A response was received from AT&T Internet Services, which advised the IP address of 2600:1700:acaf:b000:58c3:9d3a:6ae7:9830 had been assigned to AT&T account #304963411, on the above-listed date and time, which is registered to Denise Goings, with a service address of 2418 Spencer Avenue, Overland, Missouri 63114-3237, an email addresses of "denise_tierney8612@att.net" and "jimmygoings5@gmail.com," and a telephone number of (314) 201-2326.

13. This affiant viewed the files uploaded to the concerned Google account and confirmed they contain child pornography / CSAM. A sampling of the files is as follows:

FILE #1 NAME: report_1160790947257825824

DESCRIPTION: An image file composed of a montage of images, 14 of which depict a nude prepubescent female child engaged in oral and anal sexual intercourse with a male's penis.

14. On July 5th, 2022, Sergeant Brian Shanika advised this affiant that a second related CyberTipline Report, report #115492861, had been forwarded to the Special Investigations Unit from NCMEC.

15. CyberTipline Report #115492861, which was reported to NCMEC on January 14th, 2022 at 20:30:13 hours (UTC) by Google, advised that the Google account registered with the name "Jim," verified telephone number of (314) 666-0429, date of birth of xx-xx-1998,

verified email address of "jimmygiongs50@gmail.com," and additional email address of "jimmygoings50@yahoo.com," was used to upload five (5) files depicting child pornography / CSAM to the Google Photos infrastructure using the IP address of 68.72.221.127 on September 28th, 2021 at 09:53:15 hours (UTC) and 2600:1700:acaf:b000:7584:54d3:70e8:7bd6 on December 16th, 2021 at 06:33:20 hours (UTC).

16. NCMEC reported through Geo-Lookup that the IP addresses of 68.72.221.127 and 2600:1700:acaf:b000:7584:54d3:70e8:7bd6 are listed as belonging to AT&T Uverse, and registered within the St. Louis metropolitan area.

17. On June 15th, 2022, a subpoena was sent to AT&T Internet Services for user/subscriber information, to include method and type of payment for the IP addresses of 68.72.221.127 assigned on September, 28th, 2021 at 09:53:15 hours (GMT) and 2600:1700:acaf:b000:7584:54d3:70e8:7bd6 assigned on December 16th, 2021 at 06:33:20 hours (GMT). A response was received from AT&T Internet Services, which both IP addresses had been assigned to AT&T account #304963411, on the above-listed date and time, which is registered to Denise Goings, with a service address of 2418 Spencer Avenue, Overland, Missouri 63114-3237, an email addresses of "denise_tierney8612@att.net" and "jimmygoings5@gmail.com," and a telephone numbers of (314) 201-2326 and (314) 499-805.

18. This affiant viewed the files uploaded to the concerned Google account and confirmed they contain child pornography / CSAM. A sampling of the files is as follows:

FILE #2 NAME: report_1359104300381491869 8

DESCRIPTION: An image file composed of a montage of images, four (4) of which depict a prepubescent female child inserting a green object into her vagina.

19. On July 6th, 2022, a utility services check with Ameren UE indicated active utility services for the residence located at 2418 Spencer Ave., Overland, MO 63114, were registered to

Denise Goings since September of 1999, with a listed telephone number of (314) 426-8969 and an email address of "jimmygoings50@gmail.com."

20. On July 21st, 2022, this affiant prepared a St. Louis County search warrant for the residence located at 2418 Spencer Ave., Overland, MO 63114, which was presented to and granted by Judge Virginia Lay, Division 16, of the Circuit Court of St. Louis County in the state of Missouri.

21. Later, on July 21st, 2022, this affiant, along with members of the St. Louis County Police Department's Special Investigations Unit, as well as members of the St. Louis County Police Department's Tactical Operations Unit responded to 2418 Spencer Ave., Overland, MO 63114 and executed the search warrant. During a sweep of the residence, it was discovered that one of its occupants, James Goings, was away, at an unknown location in the area of Lake of the Ozarks, Missouri.

22. During the search warrant's execution, items of evidentiary value were located in and seized from the residence, including evidence item #9, a Dell computer tower, which was located in James Goings' bedroom.

23. A forensic examination was performed on the devices seized, and approximately 2,500 files depicting CSAM were located on evidence item #9. Credentials using the Google account with the email address "jimmygoings50@gmail.com" were located on the Dell computer tower.

24. This affiant knows from training and experience that people who collect child pornography tend to keep the images and/or videos they get for extended periods of time and do not delete the images and/or videos. They tend to regard the images and/or videos as trophies and use them for sexual gratification. They also use them as bargaining tools when trading with

others. Further, this affiant knows that other individuals may delete these images and/or videos knowing that the images and/or videos can be easily acquired again.

25. This affiant knows from training and experience that people who tend to collect images and/or videos of child pornography use video and audio components to capture and record child pornography. They are also known to transfer these images and/or videos to other digital media storage devices and/or social media accounts.

26. Your affiant respectfully requests that the affidavit and search warrant be sealed so as not to compromise this on-going investigation.

CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

27. Based upon my training and experience, I am aware that child pornography distributors/collectors:

a. Receive sexual gratification, stimulation, and/or satisfaction from actual physical contact with children and/or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, whether in-person or via photographs and/or other visual media, as well as from literature describing such activity;

b. Collect sexually-explicit or suggestive materials, to include but not limited to hard-core and soft-core pornography, and whether of adults and/or of children, in a variety of media, such as photographs, magazines, motion pictures, video tapes, books, slides, drawings, and/or other visual media, which they use for their own sexual arousal and gratification. Further, they commonly use this type of sexually-explicit material to lower the inhibitions of children they are attempting to seduce, to arouse the selected child-partner, and/or to demonstrate the desired sexual acts;

c. Almost always possess and maintain their material, whether it be pictures, films, videotapes, videos, magazines, negatives, photographs, correspondence, mailing lists,

books, tape recordings, child erotica, digitally stored media, etc., in the privacy and security of their homes or some other secure location to include Internet cloud storage such as that provided by Google. Child pornography distributors/collectors typically retain pictures, films, photographs, negatives, magazines, videos, correspondence, books, tape recordings, mailing lists, child erotica, digitally stored media, and/or videotapes for many years;

d. Often correspond and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually-explicit material; and often maintain lists of names, addresses, email accounts, social media accounts, usernames, and/or telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography; and,

e. Distributors/collectors who collect sexually-oriented photographs and/or videos of minors generally prefer not to be without their child pornography and/or child erotica for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

SEARCH PROCEDURE

28. In order to ensure that agents search only the computer account and/or files described in Attachment A, this affidavit and application for search warrant seek authorization to permit employees of Google LLC to assist agents in the execution of this warrant. To further ensure that agents executing this warrant search only the computer account and/or files described in Attachment A, the following procedures will be implemented:

a. The search warrant will be presented to Google LLC personnel who will be directed to isolate the account and files described in Attachment A;

b. In order to minimize any disruption of computer service to innocent third parties, Google LLC employees and law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer account and files described in Attachment A, including an exact duplicate of all information stored in the computer account and files described in Attachment A;

c. Google LLC employees will provide in electronic form the exact duplicate of the account and files described in Attachment A as well as all information stored in the account and files to the agent who serves this search warrant;

d. Law enforcement personnel will thereafter review the information stored in the account and files received from Google LLC employees and then identify and copy the information contained in the account and files which are authorized to be further copied by this search warrant; and,

e. Law enforcement personnel will then seal the original duplicate of the account and files received from Google LLC employees and will not further review the original duplicate absent an order of the Court.

CONCLUSION

29. Based upon the aforementioned information, your affiant believes that probable cause exists that Google LLC, which is located at 1600 Amphitheatre Parkway in Mountain View, CA 94043, has evidence, as listed in Attachment A, relating to the transmission, distribution, and/or receipt of child pornography related to the following Google account: **jimmygoings50@gmail.com**.

30. Specifically, it is believed Google LLC has records regarding this account's uploaded content, downloaded content, correspondence, videos, photographs, any and all other digitally-stored media and/or content, subscriber information, terms of service violation reports,

detailed billing records, and/or any and all other content, which contain evidence of violations of Title 18, United States Code, Sections 2252 and 2252A as described in Attachment A.

I state under the penalty of perjury that the foregoing is true and correct.

DET. STOEHNER 3932

STEPHANIE STOEHNER
Special Federal Officer
Federal Bureau of Investigation

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on this 4th day of August 2023.

HONORABLE
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with jimmygoings50@gmail.com ("the Subject Account") that is stored at premises owned, maintained, controlled, or operated by Google LLC a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC ("Google")

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on October 26, 2022 with the Google Reference Number 25843556, Google is required to disclose to the government for each account or identifier listed in Attachment A the following information from **December 1, 2020** to **Present**, unless otherwise indicated:

a. All business records and subscriber information, in any form kept, pertaining to the Account, including:

1. Names (including subscriber names, usernames, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);
3. Telephone numbers, including SMS recovery and alternate sign-in numbers;
4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions, including log-in IP addresses;

5. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers

6. Length of service (including start date and creation IP) and types of service utilized;

7. Means and source of payment (including any credit card or bank account number); and

8. Change history.

b. All device information associated with the Account, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;

c. Records of user activity for each connection made to or from the Account(s), including, for all Google services, the date, time, length, and method of connection, data transfer volume, usernames, source and destination IP address, name of accessed Google service, and all activity logs

d. The content of all communications sent to or from the account (including through Gmail, Google Hangouts (including videos), and otherwise), stored in draft form in the account, or otherwise associated with the account, including all message content, attachments, and header information;

e. All address book, contact list, or similar information associated with the account;

f. Full Google search history and Chrome browser history associated with the account;

g. All Google Drive content;

h. All bookmarks maintained by the account;

i. All services used by the account;

j. All subscriber and payment information, including full name, e-mail address (including any secondary or recovery email addresses), physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, telephone number, websites, screen names, user identification numbers, security questions and answers, registration IP address, payment history, and other personal identifiers;

k. All past and current usernames, account passwords, and names associated with the account;

l. The dates and times at which the account and profile were created, and the Internet Protocol ("IP") address at the time of sign-up;

m. All transactional records associated with the account, including any IP logs or other records of session times and durations;

n. Any information identifying the device or devices used to access the account, including a device serial number, a GUID or Global Unique Identifier, Android ID, a phone number, serial numbers, MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), International Mobile Subscriber Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI"), and any other information regarding the types of devices used to access the account;

o. All activity logs for the account;

p. All photos and videos uploaded to the account, including in Google Drive and Google Photos;

q. All photos and videos uploaded by any user that have that user tagged in them;

r. All location and maps information;

s. The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

t. All privacy settings and other account settings, including email addresses or other accounts that the account has blocked;

u. Advertising and Device Data: All advertising data relating to the account, including, but not limited to, advertising cookies, information regarding unique advertising IDs associated with the user, any devices used to access the account, Android IDs, application IDs, UDIDs, payment information (including, but not limited to, full credit card numbers and expiration dates and PayPal accounts), ads clicked, and ads created;

v. Linked Accounts: All accounts linked to the Target Account (including where linked by machine cookie or other cookie, creation or login IP address, recovery email or phone number, AOL account ID, Android ID, Google ID, SMS, Apple ID, or otherwise);

w. For accounts linked by cookie, the date(s) on which they shared a cookie;

x. For accounts linked by SMS number, information regarding whether the numbers were verified; and

y. Customer Correspondence: All records pertaining to communications between the Service Provider and any person regarding the user or the user's account with the Service Provider, including contacts with support services, records of actions taken, and investigative or user complaints concerning the subscriber; and

z. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

Google is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by _____, and my official title is _____. I am a custodian of records for_____. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of _____, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of _____; and

c. such records were made by _____ as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature